**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

**March 30, 2015**

*The following cyber advisory was issued by the State of Alaska and
was intended for State government entities. The information may or
may not be applicable to the general public and accordingly, the State
does not warrant its use for any specific purposes.*

**ADVISORY NUMBER:**
**SA2015-033A - UPDATED**

**DATE ISSUED:**
**03/27/2015**
**03/31/2015 - Updated**

**SUBJECT:**
**Multiple Vulnerabilities in PHP Could Allow Remote Code Execution**

**OVERVIEW:**
**Multiple vulnerabilities have been discovered in PHP which could allow an attacker to
remotely disclose source code and potentially execute arbitrary code. PHP is a
programming language originally designed for use in web-based applications with HTML
content. PHP supports a wide variety of platforms and is used by numerous web-based
software applications.**

**Successfully exploiting this issue may allow remote attackers to execute arbitrary code in
the context of a webserver. Failed attempts will likely result in denial-of-service conditions.**

**THREAT INTELLIGENCE:**
**There are currently no reports of these vulnerabilities being exploited in the wild. There
are known exploits for these vulnerabilities.**

**SYSTEM AFFECTED:**
- **PHP 5.6 prior to 5.6.7**
- **PHP 5.5 prior to 5.5.23**
- **PHP 5.4 prior to 5.4.39**

**RISK:**

**Government:**

- **Large and medium government entities:  High**
- **Small government entities: High**

**Businesses:**

- **Large and medium business entities:  High**
- **Small business entities:  High**

**Home users: N/A**

**TECHNICAL SUMMARY:**

**Multiple remote code execution vulnerabilities were fixed in PHP versions 5.4.39, 5.5.23, and 5.6.7. These vulnerabilities include:**

**A use-after-free vulnerability due to a use-after-free error in the '_wakeup()' magic method. An attacker could exploit this issue using a specially crafted input passed to the 'unserialize()' method. Successfully exploiting this issue could allow remote attackers to execute arbitrary code in the context of a webserver. Failed attempts will likely result in denial-of-service conditions. (CVE-2015-0231)**

**A heap overflow vulnerability in regcomp.c. This is due to an error in the 'len' variable, which when enlarged, fails to perform proper bounds checking allowing for an attacker to overflow the variable and modify data in memory. Successfully exploiting this issue could allow remote attackers to execute arbitrary code in the context of a webserver. Failed attempts will likely result in denial-of-service conditions. (CVE-2015-2305)**

**A heap overflow vulnerability in ZIP. When opening a ZipArchive with a large number of entries, the data will write pass the heap boundry. Successfully exploiting this issue could allow remote attackers to execute arbitrary code in the context of a webserver. Failed attempts will likely result in denial-of-service conditions. (CVE-2015-2331)**

**Other Bugs Fixed in the PHP Core for these versions may be found below.**

**Version 5.4.39**

- **Bug 69134 – Per Directory Value overrides PHP_INI_SYSTEM configuration options.**
- **Bug 69207 – When using 'move_uploaded'file' null values are allowed in the path.**

**Versions 5.5.23 & 5.6.7**

- **Bug 69174 – Leaks when unused inner class use traits precedence**
- **Bug 69139 – gc_zval_possible_root would crash when unserializing a specific string**
- **Bug 69121 – Segfault in get_current_user when script owner is not in passwd with ZTS build**
- **Bug 65593 – When calling ob_start from an output buffer this may result in a segfault.**
- **Bug 69017 – Fail to push to the empty array with the constant value defined in class scope**
- **Bug 68986 – Pointer returned by php_stream_fopen_temporary_file not validated in memory.c**
- **Bug 68166 – Exception with invalid character causes segv**
- **Bug 69141 – Missing arguments in reflection info for some builtin functions**
- **Bug 69134 – Per Directory Values overrides PHP_INI_SYSTEM configuration options**
- **Bug 69207 – Move_uploaded_file allows nulls in path**

**March 31 - UPDATED TECHNICAL SUMMARY:**

**A use-after-free vulnerability due to a use-after-free error in the '_wakeup()' magic method. An attacker could exploit this issue using a specially crafted input passed to the 'unserialize()' method. Successfully exploiting this issue could allow remote attackers to execute arbitrary code in the context of a webserver. Failed attempts will likely result in denial-of-service conditions. (CVE-2015-2787)**

**Version 5.4.39 - 5.6.7**
• **Bug  68976 - Use After Free Vulnerability in unserialize()**

**RECOMMENDATIONS:**

**We recommend the following actions be taken:**
• **Verify no unauthorized modifications occurred to the system before installing patches.**
• **Apply appropriate fixes or patches provided by the PHP Group to vulnerable systems immediately after appropriate testing.**
• **Apply the principle of Least Privilege to all systems and services.**
• **Remind users not to visit websites or follow links provided by unknown or untrusted sources.**
• **Do not open email attachments from unknown or untrusted sources.**
• **Limit user account privileges to only those required.**

**REFERENCES:**

**PHP:**
**http://php.net/ChangeLog-5.php#5.4.39**
**http://php.net/ChangeLog-5.php#5.5.23**
**http://php.net/ChangeLog-5.php#5.6.7**

**SecLists:**
**http://seclists.org/fulldisclosure/2015/Mar/140**
**http://seclists.org/fulldisclosure/2015/Mar/141**

**INulledMyself:**
**http://www.inulledmyself.com/2015/02/exploiting-memory-corruption-bugs-in.html**

**CVE:**
**https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0231**
**https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2305**
**https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2331**

**March 31 - UPDATED REFERENCES:**

**CVE:**
**https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2787**